~~CONFIDENTIAL~~

Subject copy

File 1.4.5.

DIRECTOR OF CENTRAL INTELLIGENCE
Security Committee

SECOM-D-301

12 December 1985

MEMORANDUM FOR: Chairman, DCI Information Handling Committee

FROM: [redacted] SAISS Alternate Member, DCI SECOM Staff 25X1

SUBJECT: Proposal for NTISS Instruction (NTISSI) on the Standard for Password USAGE

REFERENCE: DCI/ICS 85-4112 dtd 22 Nov 85 (attachment B)

1. Reference was received as part of a transmittal from the executive secretary of the SAISS. She mentions that the subject proposal will be discussed at the 18 December SAISS meeting (Attachment A). [redacted] 25X1

2. [redacted] letter is totally on target with his criticism of the prohibition of password classification in a dedicated or system high mode environment. His rationale based on existing policies and his refusal to accept individual rings of security as perfect is sound. There is one additional point which could have been added, had we seen the letter in advance, pertaining to audit trails. Audit trails are rendered useless if both the USERID's of individuals and the corresponding passwords are mandated to be common knowledge within the users' group. The ability to track down suspicious activities and to resolve them as either intentional or accidental is destroyed if users can sign on as someone else in the group. Effectively then, two basic safeguards, system access control and personal accountability, are voided by one unwise rule. [redacted] 25X1 25X1

3. In my discussions with [redacted] after having seen the memorandum, one final objection was brought up. [redacted] and I agree that even if there had been some redeeming value in the password suggestion, the position on classification should not have been stated as a prohibition but rather as a "normally not necessary" or other phrase which would allow classification where warranted. Because the idea is so fundamentally bad, however, [redacted] was probably correct in not even discussing this compromise. [redacted] 25X1 25X1

4. I recommend that [redacted] discuss these additional points at the 18 December SAISS meeting. 25X1

25X1

[redacted]

25X1

[redacted]

Prepared by: SECOM/[redacted]

Distribution:
Orig - Addressee
1 - ICS Registry
1 - SECOM Chrono
1 - SECOM Subject

~~CONFIDENTIAL~~

Next 1 Page(s) In Document Denied

(A)

SAISS

SUBCOMMITTEE ON
AUTOMATED INFORMATION
SYSTEMS SECURITY

EXECUTIVE SECRETARY

SAISS-062-85
2 December 1985

MEMORANDUM FOR THE MEMBERS AND OBSERVERS, SUBCOMMITTEE ON AUTOMATED INFORMATION SYSTEMS SECURITY

SUBJECT: 18 December 1985 SAISS Meeting

1. The next SAISS meeting will be on 18 December 1985 in Room 6W02 of [redacted] from 2:00 - 4:00 pm. The classification of the meeting will be at the SECRET level. STAT

2. Enclosed for your review are (1) changes to the minutes of the 31 October 1985 meeting of the SAISS, (2) the proposed agenda for the 18 December 1985 meeting of the SAISS, (3) a proposed calendar of SAISS meeting dates for 1986, (4) a memorandum from the IC Staff on the WG#3 proposed Standard on Password Usage, (5) a note from the SAISS Executive Secretary on Password Usage, (6) a memorandum from the NTISSC Executive Secretary reminding NTISSC participants of the need to keep security clearances current, and (7) a current SAISS membership roster.

[redacted] STAT

Executive Secretary

Encls:
a/s

(13.)

DCI/ICS 85-4112
22 November 1985

MEMORANDUM FOR: Chairman, SAISS

FROM: [redacted] IC Staff

SUBJECT: Proposal for NTISS Instruction (NTISSI) on the Standard for Password Usage

REFERENCE: SAISS-055-85, 28 October 1985

1. The referenced memorandum from the chairman of working group #3 proposes that FIPS Standard 112, together with certain appendices, be submitted by the SAISS to the NTISS Issuance System for approval as an NTISS Instruction and requests comments on this proposal.

2. While we have no objection to the issuance of FIPS 112 as an NTISS Instruction, we do not believe that the Department of Defense Password Management Guideline should be included as an appendix unless this document is amended in accordance with the following comments thereon.

3. Our comments and objections concern language contained in the Appendix to the DoD Management Guideline headed "E.4". (All references herein are to the pages and paragraphs as amended for the purposes of this submission.) The first paragraph of section 2 of Appendix E-4, p. 72, as presently written states:

> "Passwords that are used in ADP systems that operate in the dedicated or system high modes should not be classified, but should be protected to the same degree as For Official Use Only information..."

This statement is contrary to Intelligence Community policies and practices for systems processing SCI and is, in our opinion, not a proper guideline for other systems processing classified information. The rationale given in the document is stated as follows:

> "In this case, there is no need to classify passwords since access to the area in which the system resides is restricted to those with a clearance as high as the highest classification level of the information processed. A person who obtained a password for a system running in dedicated or system high security mode but who did not possess the proper security clearance would be unable to gain physical access to the system and use the password."

In the real world one cannot make the assumption that physical access controls are 100% effective, particularly since this is a guideline designed to be applied to all possible cases. While the existence of good physical access controls may be deemed sufficient to not require that passwords be invariably classified at the highest level of information being processed in a system high or dedicated mode processor, even a guideline should not be endorsed and issued which, in effect, mandates that passwords in such systems not be classified. Neither should the NTISSC issue a document containing a statement of rationale which permits the assumption that physical access controls always and invariably are effective.

4. The same objections apply to the language contained in the third paragraph of section 2 of Appendix E.4.

5. Since it would be desirable to include the balance of the DoD Password Management Guideline as an appendix, we suggest that an attempt be made to work out an acceptable amendment to the objectionable language of this appendix. Failing that, consideration should be given to removing Appendix E.4 from the proposed NTISSI, or if this is not acceptable, to deleting the DoD Password Management Guideline from the proposed NTISSI altogether. We will be happy to attempt to draft some acceptable alternative wording if desired.

[redacted]

STAT